

Storm Worm returns as a New Years Greeting

* * * * * 1 Votes

Friday, January 4th, 2008 | Related entries: [Internet](#), [Security](#)



Everybody's mail inboxes must surely have been filled up with New Years wishes from friends, family and spammers alike! In case you are still opening those E-greetings, be very careful as a massive attack of the [Storm Worm](#) variant known as 'Zhelatin.pt' is doing the rounds on the Internet, say security experts at MicroWorld Technologies.

Basically, you must be aware of opening up emails with the subject line that reads 'Happy New Year' or 'Message for new year'. The mail body has a Web address chosen from a random list that contains URLs like newyearcards2008.com, newyearwithlove.com, hohoho2008.com, hellosanta2008.com, happy2008toyou.com and uhavepostcard.com.

Security experts at MicroWorld have warned all Internet users not to access any of these Web sites via their computers as well. On these sites, a message is displayed which reads as, "Your download should begin shortly..Click gere to launch the download and press Run. Enjoy!".

Once the victim clicks on the downloaded .exe, the Worm drops some files and runs certain services to quickly and silently make the computer a part of a large spam relaying network or Botnet.

According to **Manoj Mansukhani, Head - Global Marketing, MicroWorld Technologies**, "Taking down the websites used in this Worm attack is quite a challenge as all of them are hosted using a technique called Fast-Flux DNS. Fast-Fluxing is a method where Virus authors deploy a continuously changing network of botnet computers to act as proxies for hosting harmful websites. To add to it, the Russian domain name provider where these sites are registered to is closed for the first week of January, which gives ample time for the criminals behind the worm to make merry!"

The original Zhelatin variant [first appeared](#) in January 2007 and spread via emails with the subject line that read '230 dead as storm batters Europe' and other socio-political events. And, this is how the worm was named as Storm Worm.

"Storm Worm is the most successful malware of its kind with an established botnet of around 3 million compromised computers worldwide according to some estimates. This network of zombie PCs relays a significant portion of the spam mail traffic on the Internet today.

Unlike most other botnets, this one does not have a central command but operates using peer-to-peer networks which makes it practically impossible to dismantle it," Manoj points out.

In order to protect their computers from Storm Worm, users must resist the temptation of clicking on a season's greetings message from an unknown source and one that requires them to visit unknown Web sites and to download files.

It is also very important to keep your AntiVirus and Spam Control systems updated, concluded Manoj.

submit Storm Worm returns as a New Years Greeting to slashdot.com

[RSS](#) | [Permanent Link](#) | [Del.icio.us](#) | [Cosmos](#) | [Digg](#) | [Slashdot](#)
| You can skip to the end and leave a response. Pinging is currently not allowed.

Related:

- [Storm Worm Botnet now Targets Barclays Customers With Phishing Attacks](#)
- [‘Storm Worm’ Email Virus returns, raising fears of fresh Spam Flood](#)
- [Storm Trojan Worm evolves and creates Havoc on the Internet, warns SecureWorks](#)
- [Early Threat Prevention Signatures against Fast-Spreading ‘Happy New Year’ Worm deployed by SonicWALL](#)
- [Storm Worm sent 15 Million Pump-and-Dump emails in October alone](#)

« [Kingston announces Limited Edition of DT 101 2GB USB Drive, sporting a Special Design](#)
[Lenovo IdeaPad Y510, Y710 and U110 Notebooks launched](#) »

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Anti-spam word: (Required)*

To prove you're a person (not a spam script), type the security word shown in the picture.



Subscribe to comments (Email field must be filled in)

Web TechShout.com

[Subscribe to Tech Shout!](#)

Enter your email: